

1 **CLAIMS**

2 What is claimed is:

3 1. A method comprising:
4 establishing authentication information, said authentication information
5 including time information associated with authenticating logic;
6 with first logic, establishing credential information; and
7 outputting an authentication request comprising said authentication
8 information and said credential information, said authentication request being
9 cryptographically modified.

10
11 2. The method as recited in Claim 1, wherein said first logic is
12 configured to output said authentication request.

13
14 3. The method as recited in Claim 1, wherein second logic this is
15 operatively coupled to said first logic is configured to output said authentication
16 request.

17
18 4. The method as recited in Claim 2, further comprising:
19 with second logic that is operatively coupled to said first logic, receiving
20 said authentication request and outputting a selectively modified authentication
21 request.

1 5. The method as recited in Claim 1, further comprising:
2 with authenticating logic that is operatively configured to receive said
3 authentication request, at least validating said authentication information, and
4 authenticating said credential information.

5
6 6. The method as recited in Claim 5, further comprising:
7 with said authenticating logic, outputting an authentication response
8 comprising authentication approval information and corresponding cryptography
9 information.

10
11 7. The method as recited in Claim 6, further comprising:
12 with said first logic, accessing at least a portion of said authentication
13 response to retrieve said corresponding cryptography information and outputting
14 said retrieved cryptography information.

15
16 8. The method as recited in Claim 7, further comprising:
17 with second logic that is operatively coupled to said first logic and said
18 authentication logic, accessing at least a portion of said authentication response
19 and using said retrieved cryptography information retrieve said authentication
20 approval information.

21
22 9. The method as recited in Claim 6, further comprising:
23 with said second logic, accessing at least a portion of said authentication
24 response to retrieve said corresponding cryptography information.

1 10. The method as recited in Claim 9, further comprising:
2 with said second logic, accessing at least a portion of said authentication
3 response and using said retrieved cryptography information retrieve said
4 authentication approval information.

5
6 11. The method as recited in Claim 6, wherein said authentication
7 request is cryptographically modified by encryption using a private key.

8
9 12. The method as recited in Claim 11, wherein said private key is
10 associated with said first logic.

11
12 13. The method as recited in Claim 11, wherein said private key is
13 associated with said second logic.

14
15 14. The method as recited in Claim 11, further comprising:
16 with said authenticating logic, retrieving said authentication information
17 and said credential information from said authentication request using a public key
18 pair-wise associated with said private key.

19
20 15. The method as recited in Claim 14, further comprising:
21 with said authenticating logic:
22 establishing a temporary key;
23 encrypting said temporary key using said public key to form said
24 corresponding cryptography information; and
25

1 encrypting said authentication approval information using said temporary
2 key.

3
4 16. The method as recited in Claim 15, further comprising:
5 with said second logic, providing said encrypted temporary key to said first
6 logic; and

7 with said first logic, retrieving said temporary key from said encrypted
8 temporary key using said private key.

9
10 17. The method as recited in Claim 16, further comprising:
11 with said first logic, providing said retrieved temporary key to said second
12 logic; and

13 with said second logic, retrieving said authentication approval information
14 using said retrieved temporary key.

15
16 18. The method as recited in Claim 15, wherein said temporary key
17 includes a symmetric key.

18
19 19. The method as recited in Claim 8, wherein said first logic is
20 substantially provided in a first device that includes a credential gathering
21 mechanism configurable to establish said credential information, said second logic
22 is provided at least partially in a second device, and said authenticating logic is
23 provided at least partially in a third device.

1 20. The method as recited in Claim 19, wherein said credential gathering
2 mechanism is configurable to establish biometric information.

3
4 21. The method as recited in Claim 19, wherein said second device
5 includes at least one computer operatively configured as a client device, and said
6 third device includes a computer operatively configured as a server device.

7
8 22. The method as recited in Claim 19, further comprising:
9 generating said authentication information using at least one logic selected
10 from said second logic and said authenticating logic.

11
12 23. The method as recited in Claim 19, wherein said second logic
13 modifies said authentication request by including certificate information in a
14 modified authentication request.

15
16 24. The method as recited in Claim 23, wherein said authenticating logic
17 is configured to validate said authentication request based at least in part on said
18 certificate information.

19
20 25. The method as recited in Claim 5, wherein said authenticating logic
21 is configured to validate said authentication information based on at least nonce
22 data and timestamp data within said authentication information.

1 26. The method as recited in Claim 5, wherein said authenticating logic
2 is configured to authenticate said credential information by logically comparing
3 said credential information with stored credential information.

4
5 27. The method as recited in Claim 8, wherein said authentication
6 approval information includes an access token for use by said second device.

7
8 28. The method as recited in Claim 1, wherein said authentication
9 information includes nonce data and said time information includes timestamp
10 data.

11
12 29. The method as recited in Claim 1, wherein said authentication
13 request includes at least one type of data selected from a group of data comprising
14 identifier data, nonce data, signature data, timestamp data, and credential data.

15
16 30. A computer readable medium having computer implementable
17 instructions for causing one or more processing units to perform acts comprising:
18 establishing authentication information, said authentication information
19 including time information associated with authenticating logic;
20 outputting an authentication request comprising said authentication
21 information and credential information, said authentication request being
22 cryptographically modified.

23
24 31. The computer readable medium as recited in Claim 30, wherein first
25 logic is configured to output said authentication request.

1
2 32. The computer readable medium as recited in Claim 31, wherein
3 second logic this is operatively coupled to said first logic is configured to output
4 said authentication request and said first logic is configured to provide said
5 credential information.

6
7 33. The computer readable medium as recited in Claim 31, having
8 computer implementable instructions for causing one or more processing units to
9 perform further acts comprising at least one of the following acts:

10 with second logic that is operatively coupled to said first logic, receiving
11 said authentication request and outputting a selectively modified authentication
12 request.

13
14 34. The computer readable medium as recited in Claim 30, having
15 computer implementable instructions for causing one or more processing units to
16 perform further acts comprising at least one of the following acts:

17 with authenticating logic that is operatively configured to receive said
18 authentication request, at least validating said authentication information, and
19 authenticating said credential information.

20
21 35. The computer readable medium as recited in Claim 34, having
22 computer implementable instructions for causing one or more processing units to
23 perform further acts comprising at least one of the following acts:

24

25

1 with said authenticating logic, outputting an authentication response
2 comprising authentication approval information and corresponding cryptography
3 information.

4
5 36. The computer readable medium as recited in Claim 35, having
6 computer implementable instructions for causing one or more processing units to
7 perform further acts comprising at least one of the following acts:

8 with said first logic, accessing at least a portion of said authentication
9 response to retrieve said corresponding cryptography information and outputting
10 said retrieved cryptography information.

11
12 37. The computer readable medium as recited in Claim 36, having
13 computer implementable instructions for causing one or more processing units to
14 perform further acts comprising at least one of the following acts:

15 with second logic that is operatively coupled to said first logic and said
16 authentication logic, accessing at least a portion of said authentication response
17 and using said retrieved cryptography information retrieve said authentication
18 approval information.

19
20 38. The computer readable medium as recited in Claim 35, having
21 computer implementable instructions for causing one or more processing units to
22 perform further acts comprising at least one of the following acts:

23 with said second logic, accessing at least a portion of said authentication
24 response to retrieve said corresponding cryptography information.

1 39. The computer readable medium as recited in Claim 38, having
2 computer implementable instructions for causing one or more processing units to
3 perform further acts comprising at least one of the following acts:

4 with said second logic, accessing at least a portion of said authentication
5 response and using said retrieved cryptography information retrieve said
6 authentication approval information.

7
8 40. The computer readable medium as recited in Claim 35, wherein said
9 authentication request is cryptographically modified by encryption using a private
10 key.

11
12 41. The computer readable medium as recited in Claim 40, wherein said
13 private key is associated with said first logic.

14
15 42. The computer readable medium as recited in Claim 40, wherein said
16 private key is associated with said second logic.

17
18 43. The computer readable medium as recited in Claim 40, having
19 computer implementable instructions for causing one or more processing units to
20 perform further acts comprising at least one of the following acts:

21 with said authenticating logic, retrieving said authentication information
22 and said credential information from said authentication request using a public key
23 pair-wise associated with said private key.

1 44. The computer readable medium as recited in Claim 43, having
2 computer implementable instructions for causing one or more processing units to
3 perform further acts comprising at least one of the following acts:

4 with said authenticating logic:
5 establishing a temporary key;
6 encrypting said temporary key using said public key to form said
7 corresponding cryptography information; and
8 encrypting said authentication approval information using said temporary
9 key.

10
11 45. The computer readable medium as recited in Claim 44, having
12 computer implementable instructions for causing one or more processing units to
13 perform further acts comprising at least one of the following acts:

14 with said second logic, providing said encrypted temporary key to said first
15 logic; and

16 with said first logic, retrieving said temporary key from said encrypted
17 temporary key using said private key.

18
19 46. The computer readable medium as recited in Claim 45, having
20 computer implementable instructions for causing one or more processing units to
21 perform further acts comprising at least one of the following acts:

22 with said first logic, providing said retrieved temporary key to said second
23 logic; and

24 with said second logic, retrieving said authentication approval information
25 using said retrieved temporary key.

1
2 47. The computer readable medium as recited in Claim 44, wherein said
3 temporary key includes a symmetric key.
4

5 48. The computer readable medium as recited in Claim 37, wherein said
6 first logic is substantially provided in a first device that includes a credential
7 gathering mechanism configurable to establish said credential information, said
8 second logic is provided at least partially in a second device, and said
9 authenticating logic is provided at least partially in a third device.
10

11 49. The computer readable medium as recited in Claim 48, wherein said
12 credential gathering mechanism is configurable to establish biometric information.
13

14 50. The computer readable medium as recited in Claim 48, wherein said
15 second device includes at least one computer operatively configured as a client
16 device, and said third device includes a computer operatively configured as a
17 server device.
18

19 51. The computer readable medium as recited in Claim 48, having
20 computer implementable instructions for causing one or more processing units to
21 perform further acts comprising at least one of the following acts:

22 generating said authentication information using at least one logic selected
23 from said second logic and said authenticating logic.
24
25

1 52. The computer readable medium as recited in Claim 48, wherein said
2 second logic modifies said authentication request by including certificate
3 information in a modified authentication request.
4

5 53. The computer readable medium as recited in Claim 52, wherein said
6 authenticating logic is configured to validate said authentication request based at
7 least in part on said certificate information.
8

9 54. The computer readable medium as recited in Claim 34, wherein said
10 authenticating logic is configured to validate said authentication information based
11 on at least nonce data and timestamp data within said authentication information.
12

13 55. The computer readable medium as recited in Claim 34, wherein said
14 authenticating logic is configured to authenticate said credential information by
15 logically comparing said credential information with stored credential information.
16

17 56. The computer readable medium as recited in Claim 37, wherein said
18 authentication approval information includes an access token for use by said
19 second device.
20

21 57. The computer readable medium as recited in Claim 30, wherein said
22 authentication information includes nonce data and said time information includes
23 timestamp data.
24
25

1 58. The computer readable medium as recited in Claim 30, wherein said
2 authentication request includes at least one type of data selected from a group of
3 data comprising identifier data, nonce data, signature data, timestamp data, and
4 credential data.

5
6 59. A system comprising:
7 an authentication device having authentication logic;
8 a first device having first logic;
9 a second having second logic that is operatively coupled to said
10 authentication logic and said first logic; and

11 wherein:

12 at least one of said authenticating logic and said second logic is configured
13 to provide authentication information to said first logic, said authentication
14 information including time information associated with said authenticating logic;

15 said first logic is configured to establish credential information,

16 at least one logic selected from said first logic and second logic is
17 configured to output an authentication request comprising said authentication
18 information and said credential information, said authentication request being
19 cryptographically modified;

20 said second logic is configured to output said authentication request; and

21 said authenticating logic is configured to receive said authentication
22 request, and at least validate said authentication information, and authenticate said
23 credential information.

1 60. The system as recited in Claim 59, wherein:

2 said authenticating logic is further configured to output an authentication
3 response comprising authentication approval information and corresponding
4 cryptography information.

5
6 61. The system as recited in Claim 60, wherein said authentication
7 approval information includes an access token for use by said second device.

8
9 62. The system as recited in Claim 60, wherein:

10 said first logic is further configured to access at least a portion of said
11 authentication response to retrieve said corresponding cryptography information
12 and output said retrieved cryptography information; and

13 said second logic is further configured to access at least a portion of said
14 authentication response and use said retrieved cryptography information output by
15 said first logic to retrieve said authentication approval information.

16
17 63. The system as recited in Claim 62, wherein;

18 said first logic is further configured to cryptographically modify said
19 authentication request by encryption using a private key; and

20 said authenticating logic is further configured to retrieve said authentication
21 information and said credential information from said authentication request using
22 a public key pair-wise associated with said private key.

1 64. The system as recited in Claim 63, wherein:
2 said authenticating logic is further configured to establish a temporary key,
3 encrypt said temporary key using said public key to form said corresponding
4 cryptography information, and encrypt said authentication approval information
5 using said temporary key;
6 said second logic is further configured to provide said encrypted temporary
7 key to said first logic;
8 said first logic is further configured to retrieve said temporary key from
9 said encrypted temporary key using said private key, and provide said retrieved
10 temporary key to said second logic; and
11 said second logic is further configured to retrieve said authentication
12 approval information using said retrieved temporary key.

13
14
15 65 The system as recited in Claim 60, wherein:
16 said second logic is further configured to access at least a portion of said
17 authentication response to retrieve said corresponding cryptography information
18 and use said retrieved cryptography information to retrieve said authentication
19 approval information.

1 66. An apparatus comprising:
2 a credential gathering mechanism configurable to establish credential
3 information;
4 first logic operatively coupled to said credential gathering mechanism and
5 configured to access authentication information, said authentication information
6 including time information associated with externally operating authenticating
7 logic, and output an authentication request comprising said authentication
8 information and said credential information, said authentication request being
9 cryptographically modified.

10
11 67. The apparatus as recited in Claim 66, wherein said credential
12 information includes biometric credential information.

13
14 68. An apparatus comprising:
15 means for identifying authentication information that includes time
16 information associated with authenticating logic;
17 means for establishing credential information;
18 means for outputting an authentication request comprising said
19 authentication information and said credential information, said authentication
20 request being cryptographically modified;
21 means for receiving said authentication request;
22 means for validating said authentication request;
23 means for validating said authentication information; and
24 means for authenticating said credential information.
25